# Shift – 入门白皮书

Phantom: 分布式存储套件

1.1.0 版本

Isabella Dell - Craig Campbell - Ralf S.

2018 年 3 月 10 日

# 目录

## 摘要

纵观历史，信息审查和压制一直是人类社会的一项通病。区块链和其他分布式技术的出现掀起了一场技术革命，能够确保任何内容不会被轻易审查。存储层和表示层技术的结合使终端用户和运营商有能力保存数据而不被审查成为可能。

Shift 针对审查问题提出了解决方案，并阐述了如何通过这些新技术的组合解决这个问题。

# 1 引言

本白皮书针对 Phantom 进行了入门介绍。Phantom 是一款统一的技术套件，作为平台用于在分布式系统中托管内容。本文详述了 Shift 采用的一般技术方法，并通过定义 Shift 试图使用 Plantom 解决的问题以及描述不同技术解决问题的方法进行展开说明。

## 1.1 问题定义

当今世界，对信息自由潜在威胁最大的莫过于互联网运营商本身。服务器主机、政府以及 ISPs（互联网服务供应商）控制网络并能够通过关闭服务器、列入黑名单以及接管 DNS（域名系统）限制内容访问。现有技术尚不成熟，无法阻止这些权威机构及其对互联网进行的攻击。IPFS（星际文件系统）(Benet, 2014) 等技术已蓄势待发，将被用于创造新型分布式互联网，降低审查制度造成的威胁。

## 1.2 问题阐述

### 1.2.1 网络中立性与互联网服务供应商

ISPs 是当今几乎所有终端用户接入互联网的单一入口点。这些机构通常是私有商业实体，为其客户提供连接服务。ISPs 短期内不会消失 – 他们对互联网自由的确造成了显而易见的威胁。ISPs 操控终端用户行为的一个实例发生于本世纪初。Comcast 针对 BitTorrent（文件分享）用户实施了流量控制 (to Marlene H. Dortch, 2008; Eckersley, 2007)，阻止他们访问所选内容，即使该内容是免费获取的内容。此次针对付费客户的攻击行为应视为违反了网络中立性、以及无论来源，所有内容和应用均应可访问的原则。

网络中立性从最初就作为互联网管理的不成文概念。信息自由被认为是促进代表全人类利益的技术进步的根本需要。网络中立性的另一个潜在威胁来自于 ISP，ISP 能屏蔽、限制或阻碍其不接受的内容的访问。ISPs 可能选择对内容的高级访问收取更昂贵的费用。虽然一般不太可能绕开 ISP，但是内容供应商可以使用新型技术将内容去中心化，并以一种 ISPs 无法轻易进行审查的方式进行传播。

### 1.2.2 政府机构

政府作为一个整体，在互联网上可进行执法、反恐和情报收集。鉴于这些权力和责任，政府机构还通过司法体系被赋予诸多对互联网控制的权利。例如，在美国，具备正当搜索令 FBI 便能关闭网站或服务 (Search.usa.gov, 2018), 以便更有效地审查该网站。在某些情况下，政府机构会赋予网站新的任务，广撒网以掌握更多的证据。虽然这种类型的接管通常只适用严重的犯罪活动（丝绸之路、非法服务），但是仍然对个人自由造成了直接攻击 (Martin, 2013)。

在政策领域，存在政府攻击互联网的其他实例。2017 年 9 月，西班牙政府扣押了 ".cat" 的顶级域名供应商 (Morris, 2017)，有效授权他们对该扩展下运营的 DNS 实施完全控制。此外，政府开始强制审查支持加泰罗尼亚公投的网站，并最终阻止投票点提交投票。政府审查对今天的互联网来说是一个显而易见且现实存在的危险。新型互联网要获得发展，必须改进这些问题、保持信息的自由流通。

### 1.2.3 集中式服务器托管

服务器供应商和运营商，如亚马逊和微软，提供系统用以托管网站或其他应用。通常，这些供应商过于热衷同政府机构合作以及配合他们对服务终端的要求 (Raphael, 2009; Chen, 2017)。此外，它们在互联网生态系统中充当着集中式力量。2017 年初，亚马逊 S3 东部服务中断，成千上万的网站受到影响 (Amazon, 2018)。在这次中断故障中，许多大型网站完全无法访问，大型互联网端口停止运行。

随着互联网的规模持续扩大，这些供应商将聚集更多需要托管的用户，这种情况必将会更加频繁地发生。使用一些新型技术，如 IPFS，可能缓解这一问题，但是将网站引入 IPFS 并呈现给大众的基础设施并没有得到广泛普及。

## 1.3 解决方案

要解决网络的集中化和审查问题，必须具备一个可以删除或降低单点失效的系统或软件层。网络上存在着各种各样的失效节点 – 服务器主机、DNS（域名服务）供应商以及互联网的 WAN （广域网）连接性。很遗憾，解决 WAN 连接性超出了本文档的研究范围，但是服务器托管和 DNS 问题可通过使用 Shift 开发的名为 Phantom 的软件套件得到缓解。Phantom 是一款分层应用程序，为搭建分布化提供技术堆栈。

Phantom 为许多网站审查源提供解决方案。顾名思义，Phantom 上托管的服务可以从一个主机上消失，但是仍可从网络中的另一主机进行访问。Phantom 通过完善 IPFS 主干来创建 Shift 网络的存储层。终端用户能够使用基于区块链的空间租赁系统提交文件进行长期存储。网站运营者能够使用 Hydra 来呈现资源从而使 Shift 存储集群服务其整个网站，并使用 Jenga 保持内容活跃，如果内容被审查，Jenga 会动态地更新发现的资源。这一技术套件打造出无缝式终端用户体验，且不轻易被审查。

# 2 存储层

## 2.1 星际文件系统

Phantom 存储层包含一项名为星际文件系统的自由获取技术。IPFS 是一种点对点的超媒体分布协议 (Benet, 2014)，作为主干为众多分布式存储应用服务。它为用于实现适合于服务网络应用和其他类型内容的分布式文件系统提供了有据可查的协议。据描述，IPFS 没有中心失效点，完全点对点，意味着任何用户都能参加到系统中来。这一文件系统协议不依赖任何中央机关进行运营监管。IPFS 已做好准备，创造一个新型的、免于审查的分布式互联网基础设施。

## 2.2 实施 – Shift 存储集群

IPFS 基础设施的默认状态表现为全球共享网络。这在验证数据完整性，可用性和自定义实现细节（如获得用于运行存储节点的令牌奖励）时可能会导致问题。鉴于此原因，Shift 运行了一个私有集群。存储节点使用自定义群秘钥，确保能够只与使用相同秘钥的其他节点对话。这还能够防止 Shift 节点被用于托管和传输在 Shift 网络之外添加的内容，能够增强可靠性和性能。

为了永久存储数据，IPFS 实施了识别概念。识别内容意味着可以永久获取（或直至未识别）内容。默认情况下，识别仅适用于未被识别的单个点，但是这意味着如果设备离线，内容可能丢失。解决问题的方法是使用 IPFS 集群：运营 IPFS 后台程序的子网络（或私网），仅包含 Shift 点。

Shift 集群作为包装器在 IPFS 后台程序周围运行。它使终端用户能够一起连接到一组 IPFS 节点，这样内容就能在组内进行存储和复制。集群挑选负责人负责跟踪哪个位置有可用的内容。

Shift 集群提供 IPFS 使用的模块集群系统。这一集群系统同 IPFS 后台程序协同实现以下任务：

1. 识别、未识别、再识别发送到点的内容
2. 为通信提供 HTTP API
3. 坚持并遵循集群共识
4. 复制因子
5. 文件存储与检索

这些功能共同提供了一个可扩展的分布式存储系统，该系统完全独立于公共 IPFS 网络运行。这对于允许用户在系统内插入和保存内容至关重要。

### 2.2.1 文件识别

在 IPFS 运行期间，未使用的文件在一段时间内自然会被清理。为了实现永久保存，文件必须在系统内被识别。识别能够防止垃圾搜集程序过早地删除项目，确保项目始终在集群内可用。

### 2.2.2 HTTP API

IPFS 提供了一套内部命令和功能，与网络互联互通。同一套功能集会镜像到 HTTP API，允许外部软件与系统相互作用。这些功能使 Phantom 与 IPFS 能够进行远程通信，而无需终端客户加入集群。

### 2.2.3 共识

IPFS 集群需要节点间达成共识，以确保所有存储的信息保持同步。这对已识别内容来说尤为重要，必须永久存储。一个节点挑选作为负责人并依此运行，直至离线或挑选出新的负责人。

#### 2.2.4 复制因子

Shift 托管集群当前配置为：将每条内容复制到冗余节点以防止数据丢失。这意味着每个文件在主位置外的多个其他位置均有备份。如果其中一个备份位置不可用，集群将自动复制内容到其他节点。这样就可以扩展网络，因为数据不需要被复制到每一个节点。

#### 2.2.5 文件存储与检索

一旦数据在系统内得到识别，参与节点接收传输数据，存储节点将该数据保留在集群内。当该数据的请求从服务节点到达存储节点时，存储节点将数据提供给服务节点，服务节点会缓存数据以防止重复检索相同数据。新的服务节点可以加入并从存储节点提供数据。

可通过加密哈希从系统检索文件。这些哈希在文件被插入系统时产生并保存以供后续使用。这对于使用区块链存储文件来说特别重要，因为这一哈希能提供识别符，将文件地址链接至付费存储的交易。

### 2.3 服务层

Phantom 提供了一个在存储层服务之上运行的服务层。这些服务包括 HAProxy 和 Jenga。服务层的主要功能是将 Phantom 连接至" 旧世界" 的互联网协议，例如 DNS，并为存储层提供流量管理。

#### 2.3.1 HAProxy

Phantom 包括 HAProxy，为 IPFS 及其集群的 API 端点提供离散寻址和流量管理。除了管理后端流量，HAProxy 还能管理系统的任何前端请求。它利用 SSL 提供客户和服务器间的加密通信。还负责处理所有传入请求，将其转发至后台设备或集群。有了 HAProxy 作为防御，只有白名单中的请求才能被目标应用执行。所有禁止请求都将被拒绝。

#### 2.3.2 Jenga

因为目前尚没有主流浏览器天然支持 IPFS，所以需要有一种方法将传入请求规划至特定服务器。使用谷歌或火狐浏览器扩展，选择一个 IPFS 节点服务于浏览器中的内容可以解决这个问题，但并不理想，因为终端用户不应必须安装第三方软件才能访问 Phantom 托管的网站。另一个可行的解决方案是使用内部负载平衡器，但这也存在问题。首要问题是集中化。如果负载平衡器失效，所有对 Phantom 的请求均会失效。第二个问题出现在吞吐量或性能问题上，例如当系统不得不扩大规模以处理更多流量时，系统会被要求支持整个 Phantom 网络的吞吐量，这对一个全球范围内的文件存储系统来说并不可行。

Jenga 通过提供可扩展的解决方案解决了这两个问题，该解决方案无需为最终用户查看内容安装任何附加软件。

Jenga 是一款 DNS 监控解决方案，Jenga 是一款 DNS 监控解决方案，可以观察顶级 DNS 条目以进行更改并记录这些更改。当发现与 IPFS 集群相关的更改时，Jenga 会更新集群中的所有存储节点。通过维护所有节点的持续通信，Jenga 可以就健康的 DNS 状态达成共识，随后从系统中驱逐不合格的节点。这就防止攻击者加入集群并注入不适当 DNS 条目，将 DDoS（分布式拒绝服务）攻击向量从系统中删除。

Jenga 仅依赖于 DNS 记录便搭建起分布式网络和传统网络之间的桥梁。Jenga 基于系统中存放的记录创建了动态网络寻址系统，促进了从一个节点到数千个节点的流量分级。这一功能对终端用户是透明的，无需外部交互操作。作为基础阶段，Jenga 能够使系统解决一些中心失效点：DNS 审查和流量控制。

为使 Jenga 发挥其功能，必须要求与所有 IPFS 集群中的已连接点保持连接。如果侦测到集群中出现更改，Jenga 便会使用最新信息更新 DNS。如果节点表现异常或离线，Jenga 将采取行动，将对等点的分配 CNAME 记录删除，进而将其逐出集群。对等点能够在纠正错误并向 Jenga

报告健康状况后重新加入系统。

当外部参与者的要求被传送至网关，集群会挑选一个对等点向呼叫者提供数据。这一过程通过整个集群的数据复制无缝完成。

为了使新网站加入系统，运营商必须为指向网关的域名提供 CNAME 记录。如果运营商不想使用网关，可以创建指向自己网关的 DNS 记录。数据仍将从集群进行传输，但是该站点将错失 Phantom 网关的一些优势，其主要优势是保证所有可用于服务的健康节点都被利用。

# 3 安全区块链

在分布式系统中，内容安全为重中之重。任何传入的数据在传出时都必须未经篡改，且客户需要能够信任其真实性。Phantom 利用区块链技术保证系统内部的不变性和真实性，因为不可证伪的账本能够消除许多信任相关的问题。

## 3.1 股份授权证明

Shift 被描述为经过股份授权证明保障的分布式区块链。挑选出的 101（数字 N 目前是 101）个代表元作为系统的保管人。这些代表元每 27 秒（区块时间）就会在其分配槽内产生区块，并为 Shift 的网络托管平台提供交易终结的账本。除了跟踪账户余额和注册状态，它还能提供私人和公共秘钥间的加密链接系统。

系统中的每个用户能够拥有并使用一个或多个私钥，这些私钥可被用于提供该系统内的代币所有权。这一点在与托管 Phantom 的区块链结合时尤为重要。用户需要从 Shift 区块链向 Phantom 侧链发送一些代币。

## 3.2 Phantom 侧链

侧链是与主链共存的区块链。在这种情况下，Phantom 将有一个与 Shift 主链勾连的侧链，该主链为 Phantom 提供了标记化的主干。

在 Phantom 侧链范围内，有一个独立账本会跟踪终端用户的代币余额。这些代币为用户提供了在 IPFS 群集内识别或取消识别内容的功能，并可以交换代币以长期存储文件。为了支持系统，终端用户能够作为节点运营商加入系统，并将剩余空间租赁给寻求存储的用户。

### 3.2.1 交易类型

在现有的由 Shift 提供的系统上，侧链将实行平台特定的新功能。新功能对 Shift 内的交易类型概念进行了扩展，并将创造一组新的交易类型供在侧链中使用。

类型 10 – 存储请求
终端用户或系统需要将内容存储于集群内。为此，用户会提交请求实现集群内的安全存储。当接收到侧链并确认进入区块链时，用户将被分配到系统内的存储。该存储将使用户能够将文件插入系统。

类型 11 – 返还存储
在某种情况下，用户可能不再需要使用存储。这时，用户将提交此类请求以解锁代币。交易确认后，用户将收到系统退回的代币。

类型 12 – 提供存储
为使系统正确运行，必须向系统提供存储。拥有超量存储的用户能通过提交请求将存储（包括添加的存储量）提供给网络，并且必须有权益证明支持请求。

类型 13 – 撤回存储
正如类型 11，用户可能想要退回代币，进行业务结算并向网络提供存储。用户需要向网络提交请求，一旦确认，锁定代币连同存储委托将一同被退回给用户。

## 3.3 外部交互作用 – 部署

Phantom 通过 Shift 主链应用界面进行部署。为了使运营商部署 Phantom 供自己使用，运营商需要运行 Shift 主链的副本。另外，运营商需要使用 Phantom 界面上传他们自己的文件，或使用提供的 APIs 套件插入新内容。Phantom 的自我部署对于最终用户与系统进行交互不是必需的。

# 4 表示层

与许多分层应用一样，终端用户与顶层或表示层相互作用。在 Phantom 中，表示层由 Hydra 组成，并与存储和服务层协同工作。

## 4.1 Hydra – 内容管理系统

内容管理系统是一种网络应用，用于发布文档和网站内容，无需技术知识。终端用户能够提交纯文本，软件将呈现一致的布局。具有动态内容且经常更新的网站离开 CMS 很难运行。为了克服 IPFS 的一些局限性，例如无法运行一些常见的服务器端语言写入的软件以及对许多数据库系统缺乏支持等，自定义 CMS 因此得以创建。

自定义 CMS 被称为 Hydra，是一项作为 IPFS 上建立的 CMS 运行的新技术。Hydra 同 Phantom 文件管理器协同工作，目前能够处理大部分常见任务，例如添加、修改以及删除内容。基础功能设置将满足大多数用户服务需求，开放源代码库能够让开发商自定义并根据各自需求完善软件。Hydra 写入可延展到终端客户并且其代码库为模块式设计。例如，一个网页和博客拥有相同的绘制引擎，但是可能采用不同架构。通过明确一些配置项，使用 Node.js 以编程形式创建新模块。结果文件能够只通过 IPFS 提供，所有转列均发生在客户端。

前端和后端组件独立分开。这使得开发人员能够使用他们首选的框架，例如 Vue、React 或 Angular。数据文件和模块结构被写入 JSON 文件，可连同外部系统，如 Wordpress API 一起使用。

## 4.2 Phantom UI – 文件管理器

Phantom 用户界面配备智能文件管理界面，使终端用户能够查看并修改系统管理的内容。终端用户通过使用 Shift 账户跟踪各自的内容。内容提交请求与此账户配对，用户可以从任何系统进行访问。这使得网络可以在文件发表后将文件和文件更改呈现出来。

用户能够以典型现代操作系统相同的方式管理存储内容。每一位用户采取的操作都将被传播到集群。界面提供高阶代码编辑器，所有常用文件类型拥有完整的语法高亮显示。

IPFS 为每一个数据文件创建了独一无二的哈希，能够防止托管或上传同一内容。这一功能简化了上传过程，因为可以在提交前识别重复文件。此外，这一功能使系统有效运行并减少终端用户和运营商的宽带使用。

Phantom UI 包含 DNS 向导程序，用于通过使用 Shift 托管存储集群控制托管域名的寻址。这一功能可以消除要求内容提交者托管其系统而导致的单一故障点。Phantom 使用 Jenga 填充健康节点列表，该节点列表将为请求的域提供内容。

## 4.3 内容检索

存储在系统中的数据是在内容级别而不是位置级别进行的。这一新方法具备很多优点。主要优点是数据位置不再相关，允许许多节点呈现相同的信息，并且当数据发生改变时，会产生新的哈希。将这些优点结合起来创建一个 merkle 哈希（根）和一个子文件夹或文件的相对路径，文件系统将变得更加智能。

网站地址通过 URL 定址，内容通过哈希取得。域名解析系统使用可变哈希。终端用户可使用私钥结合不可变哈希更新可变哈希。这一功能不要求域名记录更新就能做到内容更新。

# 5 安全层

在任何系统中，安全性都是重中之重。对于一个分布式系统而言，安全是创建稳定性以及建立运行信任的基础必要因素。

## 5.1 Shift 集群安全

集群在 Phantom 内起到非常重要的作用。在集群内，有多个用于托管的鉴别交换机制。这样的部署是为了保证集群安全免受攻击以及本文档未涉及的其他威胁。

鉴定的第一层在区块链层完成。用户将需要在区块链上发送类型 12 交易，注册委托的存储量，来完成注册程序。一旦这一步完成，用户便能够在 Phantom 上注册为集群参与者并完成加入程序。

在第二层，要求用户使用用于注册区块链的私钥以及存储集群的加密加入秘钥启动应用。随后，应用将在区块内搜索关联存储委托并确认其合法性。然后，应用将注册 Phantom，解码发行的秘钥并允许用户加入集群。

### 5.1.1 防止超额认购

为防止超额认购，集群和区块链承诺的存储配额会被系统严密监控。当存储可用性低时，加入和服务数据的激励就更多，因为希望向集群中插入数据的用户将支付更高的费用以使用集群。一段时间后，用户对持续存储量的需求和运营商的供应量应该均衡。

运营商将在设定时间框架内提供存储，在合约到期前允许在任何时间更新或添加。如果运营商在委托的时间框架终止前停止操作，他们将失去股权。这要求运营商保持较高的运行时间以维持系统运行。每一个区块链集群运营商都将有固定小时数的离线时间。

如上所述，运营商操作不当会受到惩罚。资金减少是一个极大的威慑，足以应对运营商行为不当的情况。用户行为不当还包括超额订购或网络泛洪。此类不当行为会导致股份资金的暂时冻结。

恶意用户行为的处理方法是限制其在一定时间内向系统提交内容的数量。用户在此期间能够完成一定数量交易，在超过限制数量后，他们发起交易的成本开始大幅增加。

## 5.2 数据保密

进入系统的内容的安全性同保护系统安全本身同样重要。用户在提交存储前有机会加密任何数据。然而，必须注意，任何加密的内容都只能通过密钥来读取。因此，用户在加密内容时必须保持谨慎并恰当保护其秘钥。

在 Phantom 中，用户向特定的收件人加密内容，而不是靠记忆加密。Phantom 可以提供一份公钥列表，用于创建包含解密密钥的加密消息，加密消息仅有接收方的私钥才能解密。

## 5.3 非法内容

在分布式系统中，非法内容总是作茧自缚。对 Phantom 来说，将不允许托管严重非法的内容。如果发现用户向系统注入非法内容，他们将会面临失去股份的风险并可能删除该内容。系统只会维护识别的内容，未识别内容将被迅速清除。这一点至关重要，因为在这种情况下，运营商的权利必须受到用户的保护。

# 6 结论

Phantom 是世界上第一个由区块链支持的分散存储应用程序之一。它在 Shift 区块链之上作为侧链和分布式应用程序实施。通过利用 IPFS 和集群，Jenga 和 Hydra，Phantom 为网络托管和内容交付提供了一个审查抵制平台。

# 参考文献


Amazon. (2018). *Summary of the amazon s3 service disruption in the northern virginia (us-east-1) region.* Retrieved from https://aws.amazon.com/message/41926/ (accessed January 31, 2018)

Benet, J. (2014). *Ipfs - content addressed, versioned, p2p file system.* Retrieved from https://filecoin.io/filecoin.pdf (accessed January 31, 2018)

Chen, C. (2017). Tired of dmca, riaa now seeks isp cooperation in catching and stopping copyright infringement. *Privacy News Online.* (https://www.privateinternetaccess.com/blog/2017/02/tired-dmca-riaa-now-seeks-isp-cooperation-catching-stopping-copyright-infringement/ (accessed January 31, 2018))

Eckersley, P. (2007). *Comcast is also jamming gnutella (and lotus notes?).* Retrieved from https://www.eff.org/deeplinks/2007/10/comcast-also-jamming-gnutella-and-lotus-notes (accessed January 31, 2018)

Martin, J. (2013). Lost on the silk road: Online drug distribution and the 'cryptomarket' . *SAGE journals.* (http://journals.sagepub.com/doi/abs/10.1177/1748895813505234 (accessed January 31, 2018))

Morris, D. (2017). Spanish polish raid .cat admin offices, threatening the internet' s cutest domain name. *Fortune.* (http://fortune.com/2017/09/23/spanish-dot-cat-domain-name/ (accessed January 31, 2018))

Raphael, J. (2009). Isps join riaa' s fight against piracy: Is your isp one of them? *PCWorld.* (https://www.pcworld.com/article/161978/riaa.html (accessed January 31, 2018))

Search.usa.gov. (2018). *Seize domain names - immigration and customs enforcement (ice) search results.* Retrieved from https://search.usa.gov/search?affiliate=ice.gov&query=seize+domain+names&commit=Search (accessed January 31, 2018)

to Marlene H. Dortch, Z. K. A. (2008). *In the matter of formal complaint of free press and public knowledge against comcast corporation for secretly degrading peer-to-peer applications, file no. eb-08-ih-1518.* Retrieved from https://ecfsapi.fcc.gov/file/6520169715.pdf (accessed January 31, 2018)